DETAILED ACTION

1.   Claims 1 – 16 are pending.

Response to Arguments

2.   Applicant's arguments with respect to claims 1 and 12 – 15, have been considered but are moot in view of the new ground(s) of rejection, as necessitated by amendment by applicant on 08/15/2008.

Claim Rejections - 35 USC § 103

3.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4.   Claims 1, 9 and 12 – 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gray U.S. Patent No. (5,844,497) in view of Laage et al. U.S. Patent No. (6,931,382) and Sankaran et al. U.S. PG-Publication No. (2002/0133444).

5.   As per claims 1 and 12 – 15, Gray teaches a process at the client data processing system applying the cipher function to the client password, which corresponds to the stored cipher-protected client password, thereby to generate a cipher-protected client password, which is equivalent to the stored cipher-protected client password (Gray, Col. 5 Lines 29 - 40, encrypted passwords), wherein the authentication method is adapted to function without additional software infrastructure

(Gray, Col. 5 Lines 29 - 40, no external software needed), but fails to teach performing

an authentication check using the client data processing system's cipher-protected

client password and the server data processing system's stored cipher-protected client

password as a shared secret for said authentication check and the client password is

never in a cleartext format on the server data processing system. However, in an

analogous art Laage teaches performing an authentication check using the client data

processing system's cipher-protected client password and the server data processing

system's stored cipher-protected client password as a shared secret for said

authentication check (Laage, Col. 10 Lines 50 – 57, hashes password to compare to

hash value stored by server) and Sankaran teaches the client password is never in a

cleartext format on the server data processing system (Sankaran, Paragraph 0047, only

hash value of password is stored).

　　　　At the time the invention was made, it could have been obvious to a person of

ordinary skill in the art to use Laage's payment instrument authorization technique with

Gray's method for providing an authentication system because it offers the advantage of

checking to see if a password is actually valid (Laage, Col. 10 Lines 50 – 57).

　　　　At the time the invention was made, it could have been obvious to a person of

ordinary skill in the art to use Sankaran's interactive method for real-time financial

planning with Gray's method for providing an authentication system because it offers

the advantage of secure remote access to users (Sankaran, Paragraph 0011).

6.　　　As per claim 9, Gray discloses the server processing system's password

repository is preferably integrated within the operating system of the server data

processing system (Gray, Col. 6 Lines 9 - 21, OS works with verification system of passwords thus accessing all passwords associated to the system).

7.   Claims 2 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gray U.S. Patent No. (5,884,497), Laage et al. U.S. Patent No. (6,931,382) and Sankaran et al. U.S. PG-Publication No. (2002/0133444) and in further view of Boyko et al. U.S. Patent No. (7,047,408).

8.   As per claim 2, Gray fails to teach an authentication check includes performing a mutual challenge-response authentication protocol check. However, in an analogous art Jablon teaches an authentication check includes performing a mutual challenge-response authentication protocol check (Boyko, Col. 3 Lines 24 - 36).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Boyko's secure mutual network authentication with Gray's apparatus for providing an authentication system, because it offers the advantage of being a more secure.

9.   As per claim 16, Gray as modified teaches generating a cipher-protected client password by applying said first cipher function to the client's password, thereby to provide the client and server processes with a shared secret (Boyko, Col. 3 Lines 24 - 36), generating a client response and counter-challenge to the server challenge, the client response and counter-challenge including a message authentication code computed using the cipher-protected client password (Boyko, Col. 3 Lines 24 - 36), forwarding the client response and counter-challenge to the server process ((Boyko,

Col. 3 Lines 24 - 36) receiving the forwarded server response; generating an anticipated

server response and comparing the received and anticipated server responses to

determine whether they match; and in response to a positive match, confirming

successful authentication (Boyko, Col. 3 Lines 24 - 36).

At the time the invention was made, it would have been obvious to a person of

ordinary skill in the art to use Boyko's secure mutual network authentication with Gray's

apparatus for providing an authentication system, because it offers the advantage of

being a more secure.

10.   Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Gray U.S.

Patent No. (5,884,497), Laage et al. U.S. Patent No. (6,931,382) and Sankaran et al.

U.S. PG-Publication No. (2002/0133444) and in further view of Patzer et al. U.S. Patent

No. (6,732,270).

11.   As per claim 3, Gray fails to teach the cipher function is an encryption algorithm

wherein the cipher-protected client password comprises a salt and a character string.

However, in an analogous art Patzer teaches the cipher function is an encryption

algorithm wherein the cipher-protected client password comprises a saltand a character

string (Patzer, Col. 4 Lines 18 - 31).

At the time the invention was made, it would have been obvious to a person of

ordinary skill in the art to use Patzer's method to authenticate a network access server

to an authentication server with Gray's apparatus for providing an authentication

system, because it offers the advantage of protecting against imposter clients (Patzer,

Co1.2 Lines 16 -20).

12.   Claims 6 – 8, are rejected under 35 U.S.C. 103(a) as being unpatentable over

Gray U.S. Patent No. (5,884,497), Laage et al. U.S. Patent No. (6,931,382) and

Sankaran et al. U.S. PG-Publication No. (2002/0133444) and in further view of Davis et

al. U.S. Patent No. (6,064,736).

13.   As per claim 6, Gray fails to teach a hash function. However, in an analogous art

Davis teaches a hash function (Davis, Col. 4, Lines 50 - 52).

        At the time the invention was made, it would have been obvious to a person of

ordinary skill in the art to use Davis' password verification method and system with

Gray's apparatus for providing an authentication system, because it offers the

advantage of protecting against unwanted users (Davis, Col. 2 Lines 15 - 26).

14.   As per claim 7, Gray as modified teaches a process at the server data

processing system retrieving from the repository the respective token for a stored

cipher-protected client password, and transmitting the token to a client data processing

system (Davis, Col. 5, Lines 11 - 14) and the process at the client data processing

system applying the cipher function to the combination of the transmitted token and the

client password which corresponds to the stored cipher-protected client password,

thereby to generate the equivalent cipher-protected client password for use as a shared

secret (Davis, Col. 5, Lines 18-31).

15.   As per claim 8 Gray as modified teaches the token is a random number (Davis,
Col. 5, Lines 11 - 13, salt).

16.   Claims 4, 5 and10 are rejected under 35 U.S.C. 103(a) as being unpatentable
over Gray U.S. Patent No. (5,884,497), Laage et al. U.S. Patent No. (6,931,382) and
Sankaran et al. U.S. PG-Publication No. (2002/0133444) and in further view of
Yatsukawa U.S. Patent No. (6,148,404).

17.   As per claim 4, Gray fail to teach an authentication check comprises generating a
common secret session key at both the client and server data processing systems,
using the generated encrypted client password at the client and the stored encrypted
client password at the server, and using this common secret session key in a mutual
challenge-response authentication protocol. However, Yatsukawa teaches an
authentication check comprises generating a common secret session key at both the
client and server data processing systems, using the generated encrypted client
password at the client and the stored encrypted client password at the server, and using
this common secret session key in a mutual challenge-response authentication protocol
(Yatsukawa, Col. 19, Lines 62 - 67).

        At the time the invention wasmade, it would have been obvious to a person of
ordinary skill in the art to us Yatsukawa's common session-key with Gray's apparatus
for providing an authentication system, because it offers the advantage of confidentiality
by limiting the chance of leakage of information between client and server, along with
unauthorized intrusion (Yatsukawa, Col. 1 Lines 35 - 42).

18.   As per claim 5, Gray teaches a secret session key is generated by applying a

cipher function to each of the generated encrypted client password at the client and the

stored encrypted client password at the server (Yatsukawa, Col. 3, Lines 52 - 55).

        At the time the invention was made, it would have been obvious to a person of

ordinary skill in the art to us Yatsukawa's common session-key with Gray's apparatus

for providing an authentication system, because it offers the advantage of confidentiality

by limiting the chance of leakage of information between client and server along with

unauthorized intrusion (Yatsukawa, Col. 1 Lines 35 - 42).

19.   As per claim 10, Gray as modified teaches the operating system is an operating

system conforming to the UNIX operating system standard or derived from a UNIX

conforming system (Yatsukawa, Col. 19, Lines 3 - 6).

20.   Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Gray

U.S. Patent No. (5,884,497) and Sankaran et al. U.S. PG-Publication No.

(2002/0133444) and Yatsukawa U.S. Patent No. (6,148,404), as applied to claim 10.

21.   As per claim 11, Gray fails to teach the encryption algorithm is provided by the

UNIX crypt() function. However, in an analogous art Davis teaches the encryption

algorithm is provided by the UNIX crypt() function (Davis, Col. 5, Lines 13 - 16).

        At the time the invention was made, it would have been obvious to a person of

ordinary skill in the art to use Davis' password verification method and system with

Gray's apparatus for providing an authentication system, because it offers the

advantage of protecting against unwanted users (Davis, Col. 2 Lines 15 - 26).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Roderick Tolentino whose telephone number is (571) 272-2661. The examiner can normally be reached on Monday - Friday 9am to 5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Roderick Tolentino
Examiner
Art Unit 2434

Roderick Tolentino
/Roderick Tolentino/
Examiner, Art Unit 2434

/Kambiz Zand/

Supervisory Patent Examiner, Art Unit 2343